WHAT IS CLAIMED IS:

1. A method of distributing cryptographic keys in a network comprising a server and a client, said method comprising:

receiving a request for a key from a client;

logging said request for said key in a log;

distributing said key to said client in response to said request;

multicasting program content for decryption by said client utilizing said key;

billing said client based upon said log.

2. The method as described in claim 1 and further comprising not monitoring whether said client requires said key prior to said receiving said request for said key.

3. The method as described in claim 1 wherein said logging said request for said key comprises:

logging a segment of said program content, wherein said key is used for decrypting said segment.

4. The method as described in claim 1 wherein said key is encrypted under a program segment key and wherein said program segment key is distributed to said client in a multicast message.

5. The method as described in claim 4 wherein said distributing said program segment key to said client comprises:

distributing said program segment key as part of a unicast message.

6. The method as described in claim 5 wherein said program segment key is encrypted under a unique key of said client.

7. The method as described in claim 4 wherein said distributing said program segment key to said client comprises:

distributing said program segment key as part of a multicast message.

8. The method as described in claim 7 wherein said program segment key is encrypted under a unique key of said client.

9. The method as described in claim 4 wherein said client is a subscriber to a service and wherein said program segment key is encrypted under a service key.

10. The method as described in claim 9 wherein said service key is distributed to said client in response to said user purchasing said service associated with said service key.

11. The method as described in claim 10 wherein said service key is encrypted under a unique key of said client.

12. The method as described in claim 1 and further comprising:

distributing a next content key in a first message wherein said next content key is encrypted under a first program segment key;

distributing said next content key in a second message wherein said next content key is encrypted under a second program segment key;

wherein said next content key is operable for decrypting a subsequent segment of said program content.

13. A method of distributing cryptographic keys in a multicasting network comprising a server and a client, said method comprising:

receiving from a client a request for a first key;

creating a list of clients that request said first key;

distributing a multicast message to said list of clients that requested said first key so as to distribute a second key, wherein said second key is for use in decrypting encrypted program content.

14. The method as described in claim 13 wherein said second key is encrypted utilizing said first key for each of said clients on said list.

15. The method as described in claim 14 wherein said first key is encrypted under a unique key.

16. The method as described in claim 13 and further comprising:

receiving a message from said client indicating that said client is leaving a multicast session.

17. The method as described in claim 16 and further comprising:

removing said client from said list.

18. The method as described in claim 16 and further comprising:

in response to said receiving said message from said client, logging an entry indicating that billing of said client should be stopped for said multicast session.

19. The method as described in claim 17 and further comprising:

distributing a third key to clients remaining on said list so as to prevent said client removed from said list from being able to decrypt a subsequent segment of program content encrypted under said third key.

20. The method as described in claim 13 and further comprising:

receiving a confirmation message from said client confirming that said client received said first key.

21. The method as described in claim 13 and further comprising:

removing said client from said list after a confirmation message is not received within a predetermined period of time after said first key is distributed.

22. A method of distributing keys in a multicasting network comprising a server and a client, said method comprising:

multicasting encrypted program content;

creating a list of active participants receiving said program, said list of active participants including said client;

receiving a message from said client indicating that said client should remain on said list of active participants;

multicasting a message to said list of active participants, said message including a new key for use in decrypting a subsequent segment of said program content.

23. The method as described in claim 22 wherein said key is encrypted with a key unique to each of said participants listed in said list of participants.

24. The method as described in claim 22 and further comprising:

removing a second client from said list of active participants if a message indicating that said second client should be maintained on said second list of participants is not received from said second client.

25. A method of transmitting a new encryption key in a network comprising a server and a client, said method comprising:

providing a packet for use as an RTP packet comprising a payload portion and a header portion;

inserting a field in said RTP packet operable to indicate key changes to said client so as to create a modified RTP packet;

transmitting said modified RTP packet to said client.

26. The method as described in claim 25 and further comprising:

receiving said modified RTP packet at said client.

27. The method as described in claim 25 and further comprising:

removing said fixed field portion from said modified RTP packet so as to recover said RTP packet.

28. The method as described in claim 25 and further comprising:

determining from said fixed field portion whether a key change occurred.

29. A method of transmitting a new encryption key in a network comprising a server and a client, said method comprising:

providing a packet for use as an RTP packet comprising a header portion;

utilizing a padding bit in said header portion to indicate key changes to said client.

30. A method of multicasting new encryption keys to a plurality of clients, said method comprising:

providing a first key for use by a first client;

encrypting said first key;

providing a second key for use by a second client;

encrypting said second key;

combining said encrypted first key and said encrypted second key as part of a message;

multicasting said message to said plurality of clients so as to allow said first client to obtain said encrypted first key and said second client to obtain said encrypted second key.

31. The method as described in claim 30 wherein said combining comprises concatenating said encrypted first key and said encrypted second key in said message.

32. The method as described in claim 30 wherein said first key and said second keys are program keys.